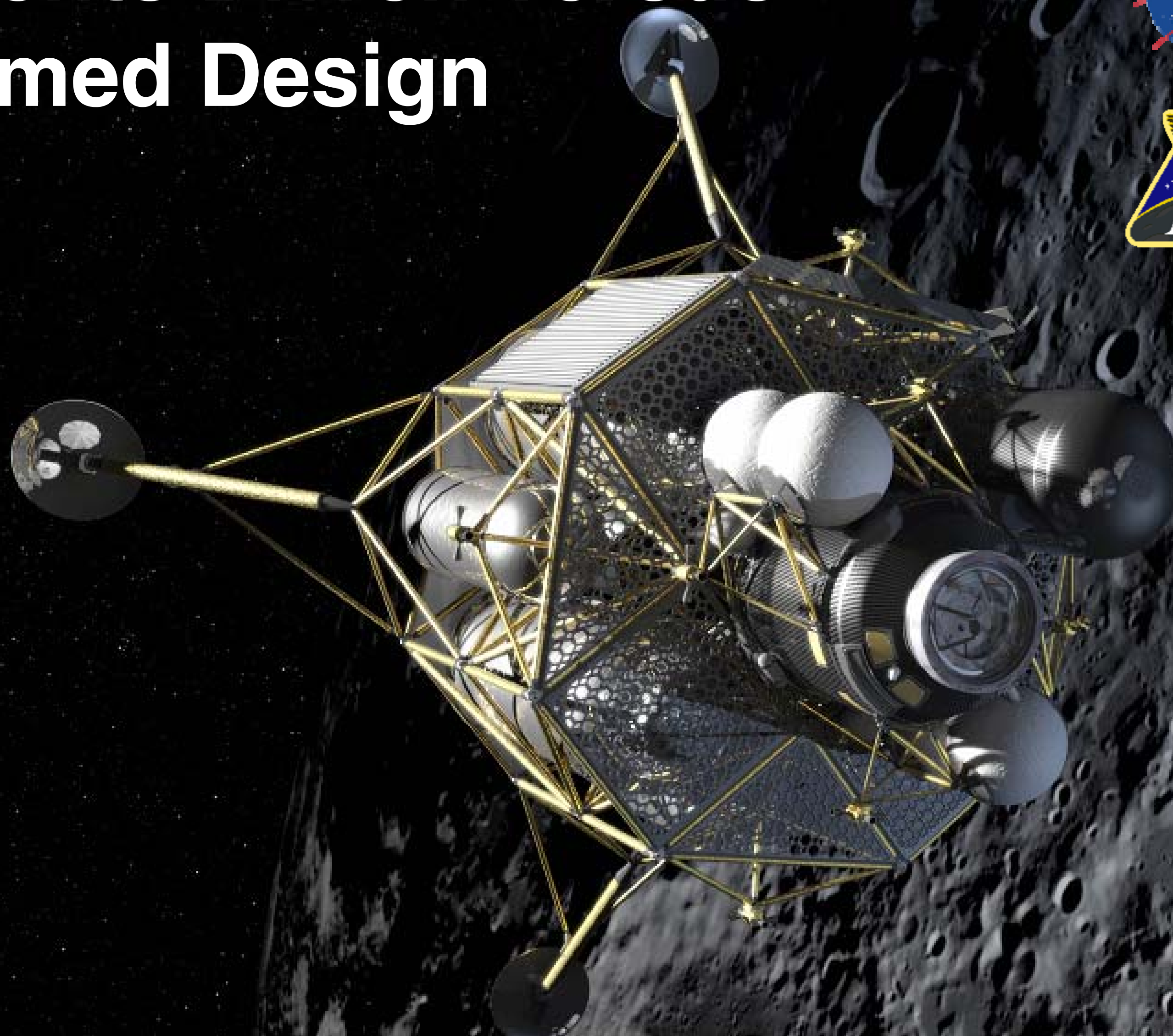
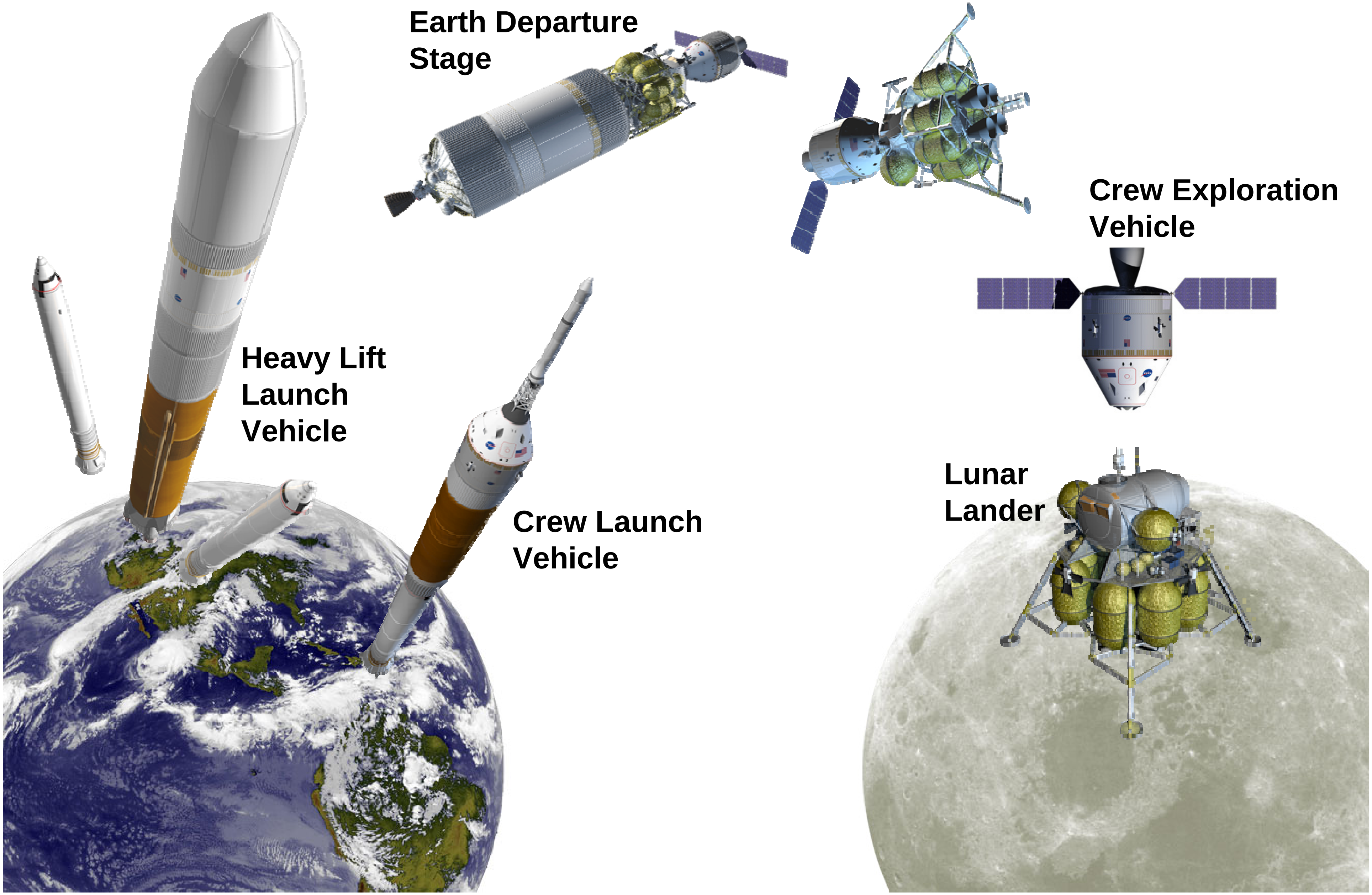
Requirements Driven versus Risk Informed Design

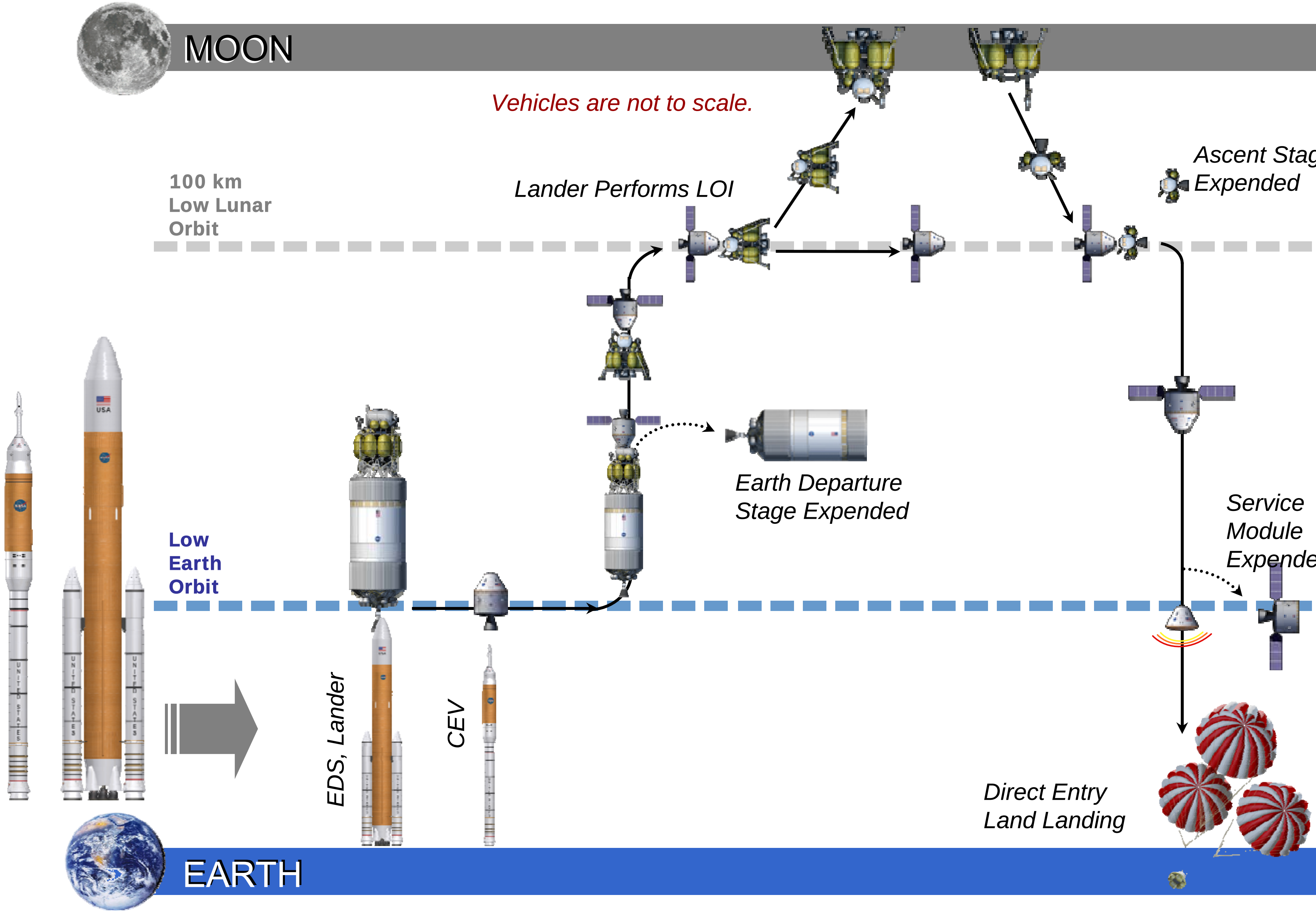


Randy Rust
SR&QA Lead,
Altair Project
Johnson Space Center

Transportation Components of Program Constellation

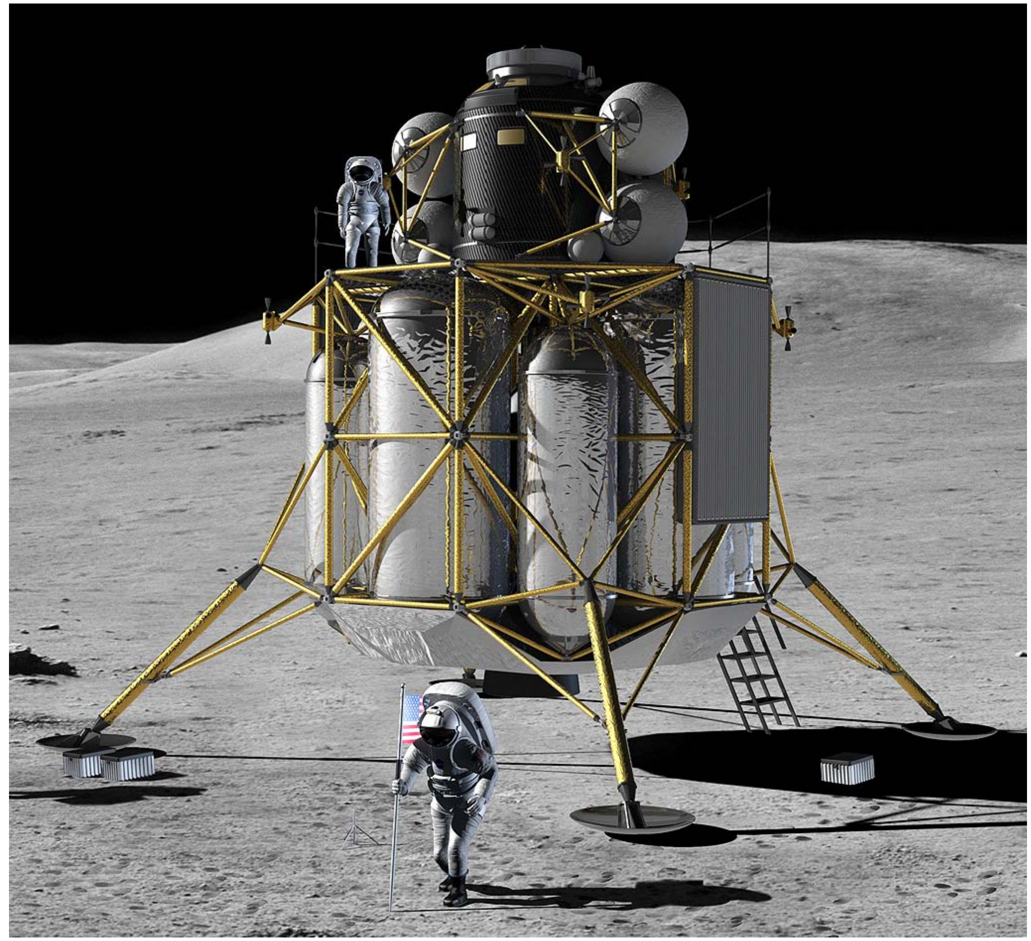


Typical Lunar Reference Mission



Altair Lunar Lander

- **4 crew to and from the surface**
  - Seven days on the surface
  - Lunar outpost crew rotation
- **Global access capability**
- **Anytime return to Earth**
- **Capability to land 14 to 17 metric tons of dedicated cargo**
- **Airlock for surface activities**
- **Descent stage:**
  - Liquid oxygen / liquid hydrogen propulsion
- **Ascent stage:**
  - Hypergolic Propellants or Liquid oxygen/methane



Design Approach

- **Project examined the multitude of concepts developed in the post-ESAS era, took lessons learned and began to develop a real design.**

- **Altair took a true risk informed design approach, starting with a minimum functionality design and adding from there to reduce risk.**

- **Lunar Design Analysis Cycle (LDAC) 1 developed a "minimum functional" vehicle.**
  - "Minimum Functionality" is a design philosophy that begins with a vehicle that will perform the mission, and no more than that
  - Does not consider contingencies
  - Does not have added redundancy ("single string" approach)
  - Provides early, critical insight into the overall viability of the end-to-end architecture
  - Provides a starting point to make informed cost/risk trades and consciously buy down risk
  - <u>A "Minimum Functionality" vehicle is NOT a design that would ever be contemplated as a "flyable" design!</u>

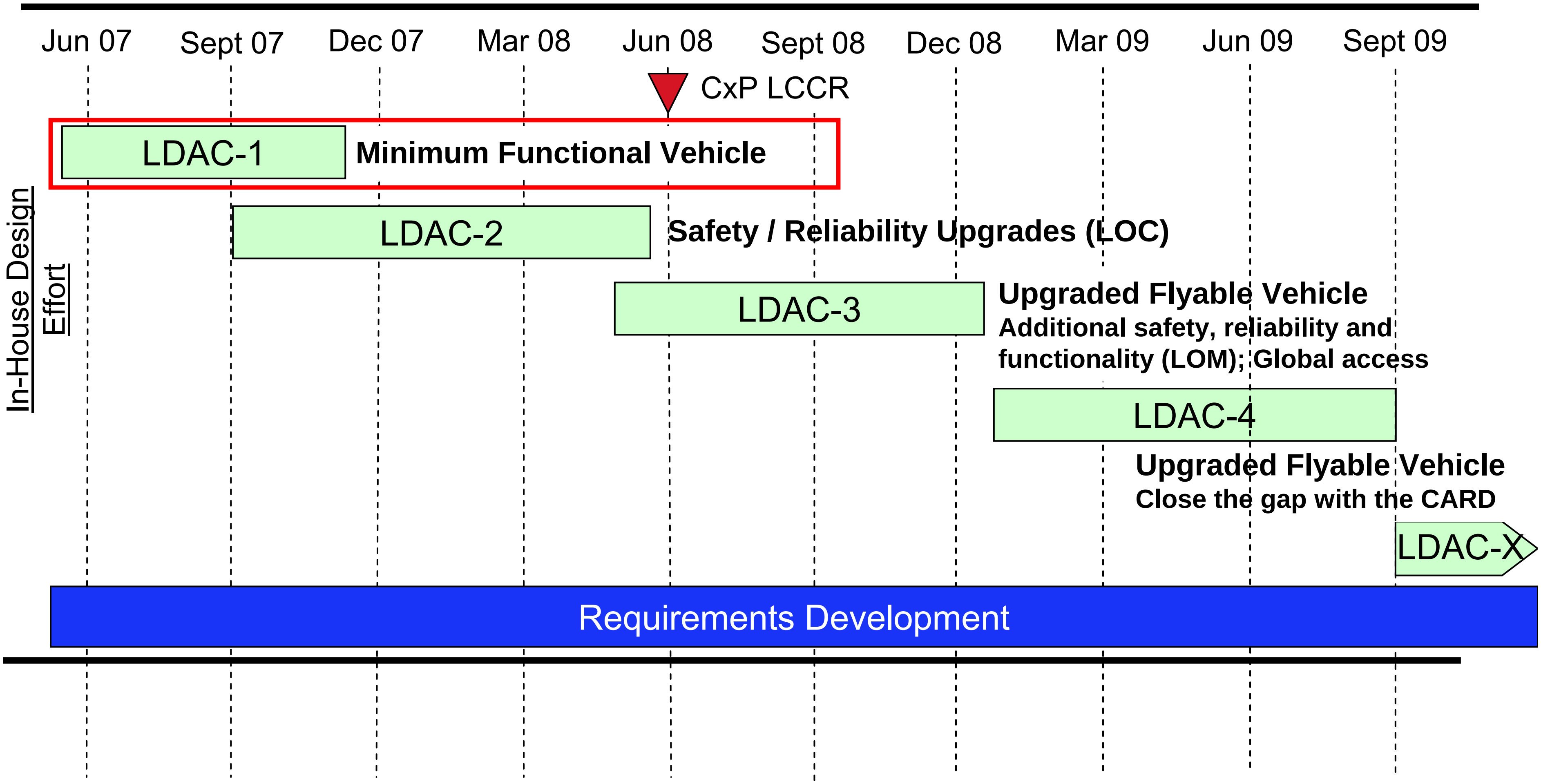
- **LDAC-2 determined the most significant contributors to loss of crew (LOC) and the optimum cost/risk trades to reduce those risks.**

- **LDAC-3 (current LDAC) is assessing biggest contributors to loss of mission (LOM) and optimum cost/risk trades to reduce those risks.**

- **Goal of the design process is to do enough real design work to understand and develop the requirements for SRR**.

Lander Design Analysis Cycle 1

- Lander design process kicked off with Design Analysis Cycle 1
- Took a "minimal functionality" approach for LDAC-1
- LDAC-1 completed November 2007



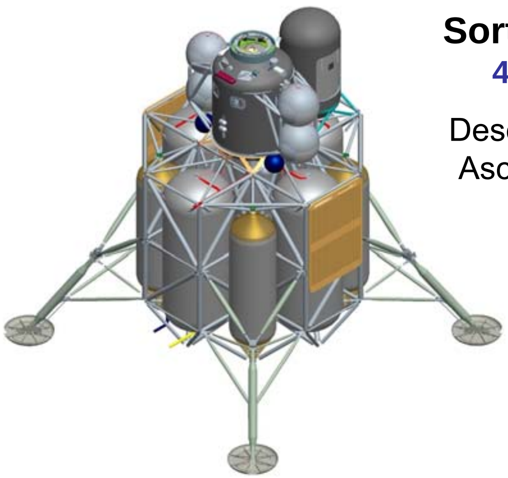
New Philosophy Needed

- For previous programs and projects, the general thought was to apply a failure tolerance philosophy
  - One failure tolerant for loss of mission failures, and two failure tolerant to prevent loss of crew.
- For the Lander, where mass is extremely critical, this philosophy alone will not yield an optimal design solution.
  - There are ways other than redundancy to improve reliability and still reduce the risk of loss of crew.
- We needed a new philosophy where we could develop a spacecraft that provides a required level of safety for the crew and is reliable enough to perform the mission.
  - Defined the minimum set of functions necessary to accomplish the mission objectives.
  - Made it work. Created the simplest & lowest mass conceptual design of the contemplated system.
  - Consistent with NESC RP-06-108, Design, Development, Test, and Evaluation (DDT&E) Considerations for Safe and Reliable Human Rated Spacecraft Systems)

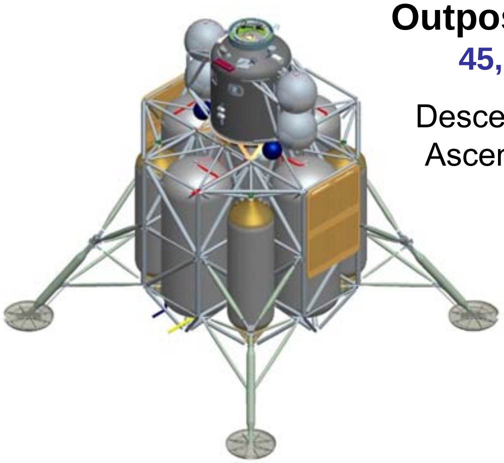
LDAC-1 Starting Point

- **'Hard' Requirements**
  - 4 Crew
  - 7 Day Sortie
  - 210 Day Outpost
  - Airlock (implemented on sortie mission only)
  - CxP transportation architecture
    - 8.4 meter shroud, TLI Loads, Lander performs LOI burn, CEV IRD, etc
  - Control Mass
    - Total Lander mass at TLI for crewed missions: 45,000 kg
    - Total Lander mass at TLI for cargo missions: 53,600 kg
- **3 DRMs with Mission Timelines and Functional Allocations**
  - Sortie Mission to South Pole
    - 4 Crew / 7 Days on Surface / No support from surface assets
    - No restrictions on 'when' (accommodating eclipse periods)
  - Outpost Mission to South Pole
    - 4 Crew with Cargo Element (LAT Campaign option 2)
    - Outpost provides habitation on surface (down and out)
    - 210 Days with surface support (power)
  - Cargo Mission to South Pole
    - Short duration, large payload
- **One Lander design, with variants (kits) if required for the different DRMs**

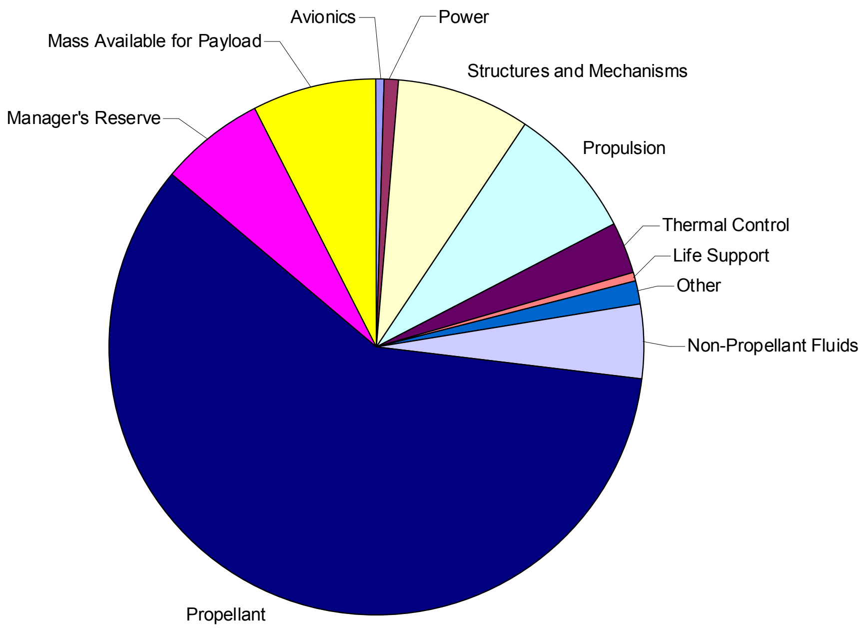
Results of LDAC1



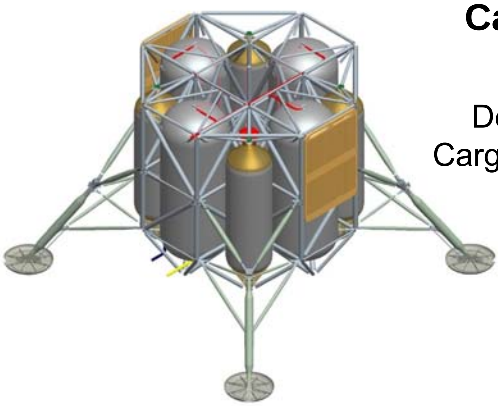
Sortie Variant
45,000 kg
Descent Module
Ascent Module
Airlock



Outpost Variant
45,000 kg
Descent Module
Ascent Module



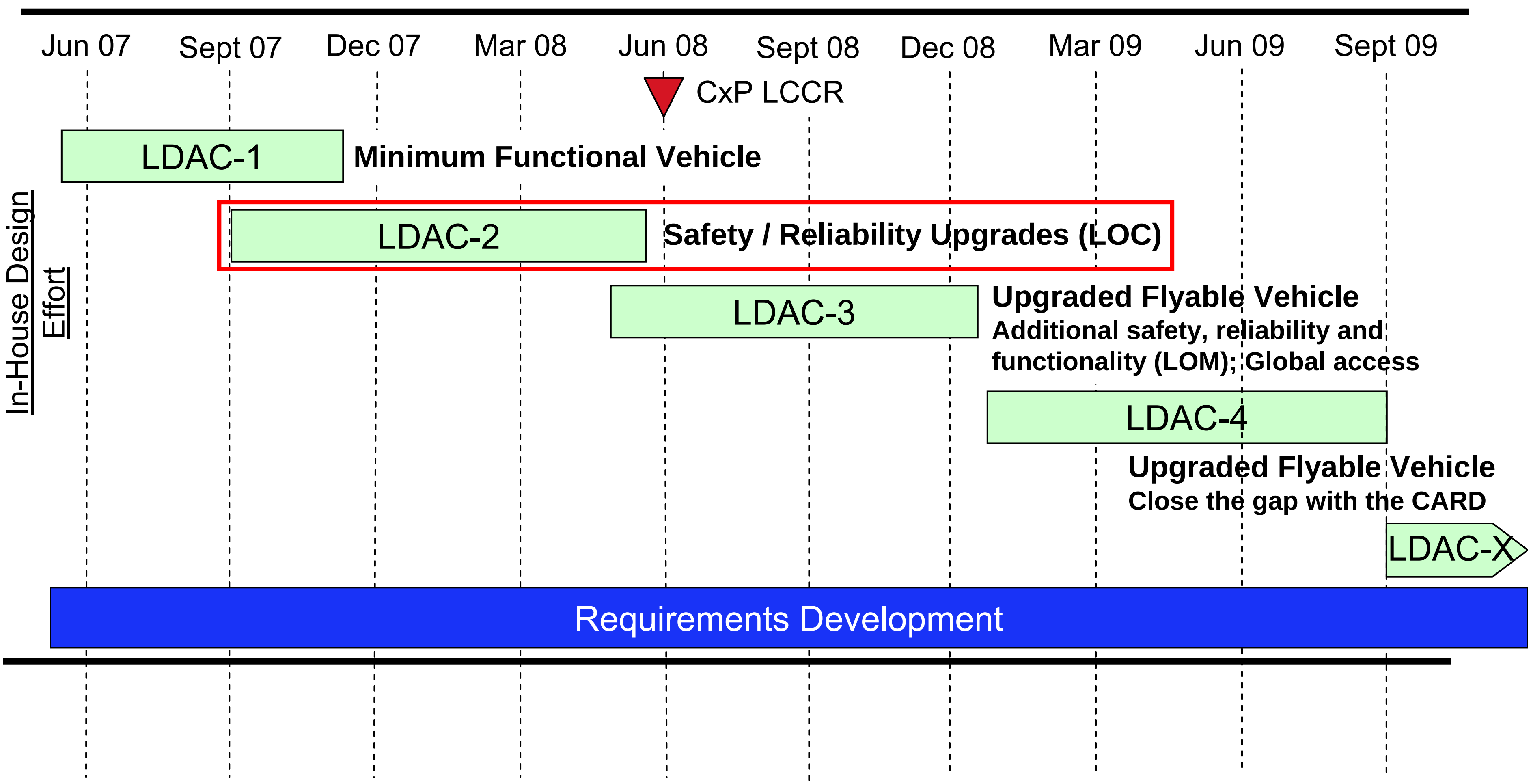
Sortie Mission Lander Mass distribution



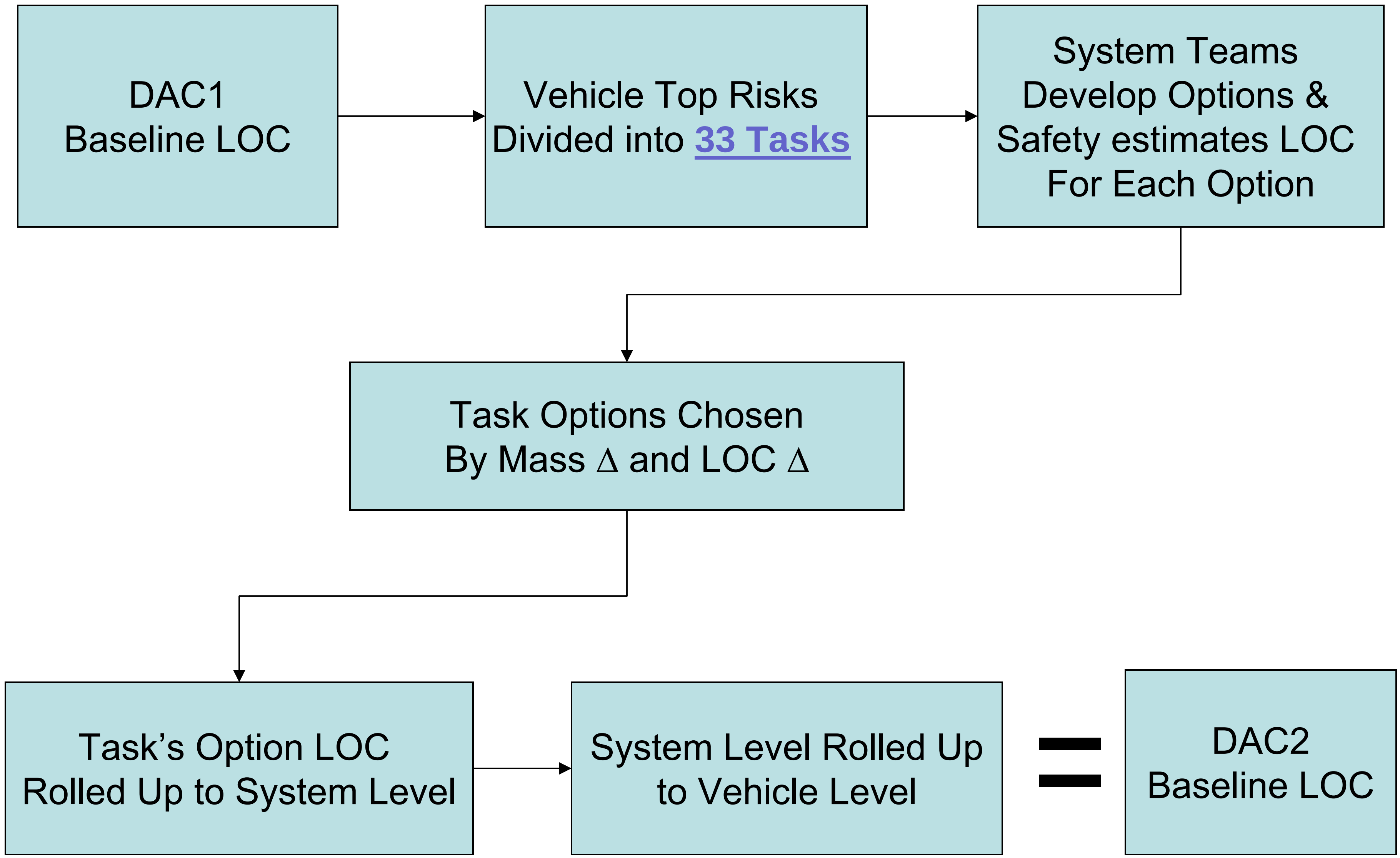
Cargo Variant
53,600 kg
Descent Module
Cargo on Upper Deck

Lander Design Analysis Cycle 2

- LDAC2's focus was to buy down the Loss of Crew (LOC) safety risks in the point of departure design.
- LDAC2 completion date was May 2008.



Overview of LDAC-2 risk buy back process



Example Risk Buyback Task:
#33, Improve Comm System Reliability

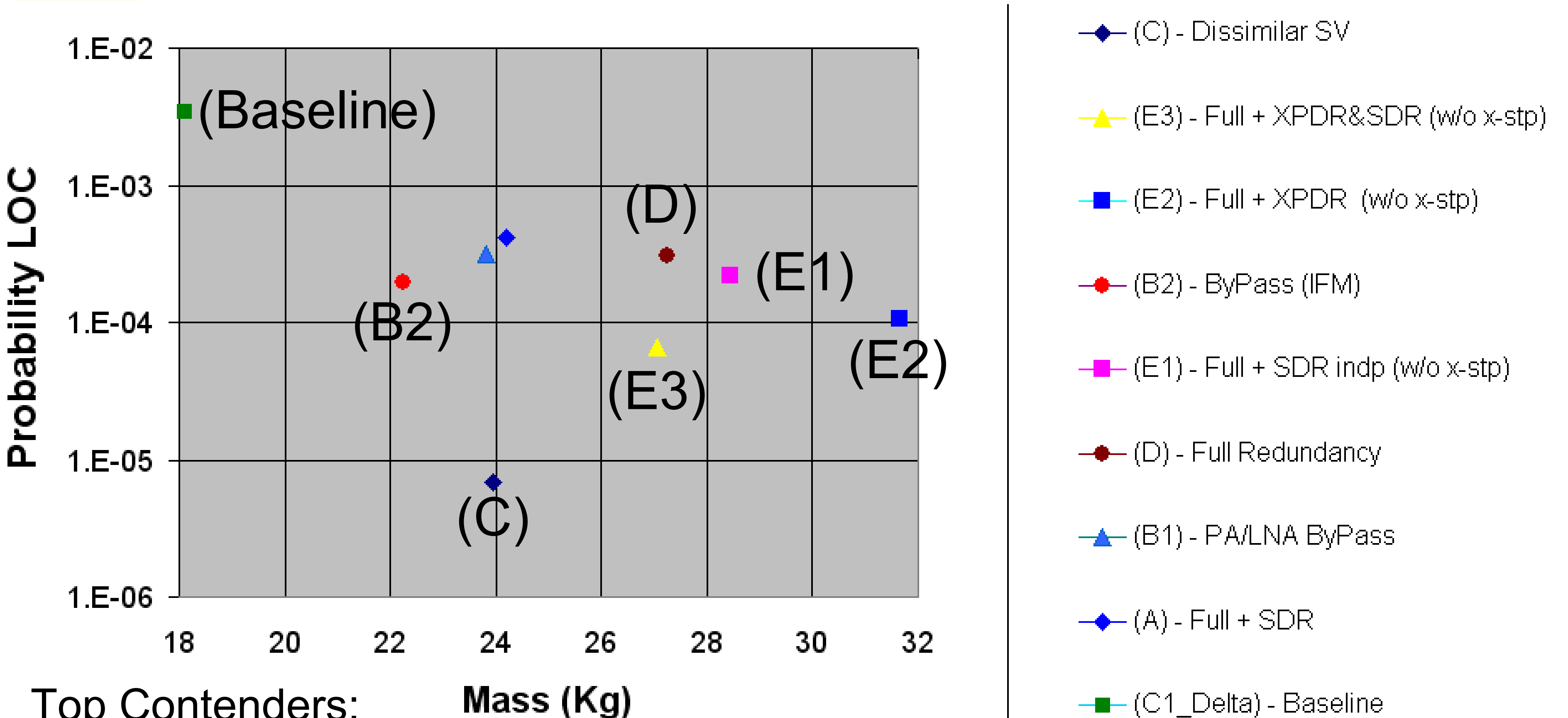
- **Purpose: Improve Comm System Reliability to be able to update the state vector**
- **Brief description of problem addressed by your task**
  - There are currently 6 single point failures that could cause loss of the state vector input to the bus to the flight computer. This study identifies several options increase communications reliability.
  - Inability to obtain state vector results in LOC for ascent.

Proposed Solutions:

- (A) Redundancy with 2 SDRs (instead of XPDR's), cross-strapped to single diplexer/antenna pair (common EVA comm)
- (B1) PA/LNA Bypass (with switches)
- (B2) PA/LNA Bypass (with cables - IFM)
- (C) Redundancy with 1 XPDR & 1 Dissimilar comm system
- (D) Redundancy with 2 XPDRs, cross-strapped to single diplexer/antenna pair
- (E1) Full Redundancy with 2 SDRs strings (common EVA comm)
- (E2) Full Redundancy with 2 XPDRs strings
- (E3) Full Redundancy, 1 XPDR & 1 SDR strings (common EVA comm)

Example Risk Buyback Task: #33, Improve Comm System Reliability

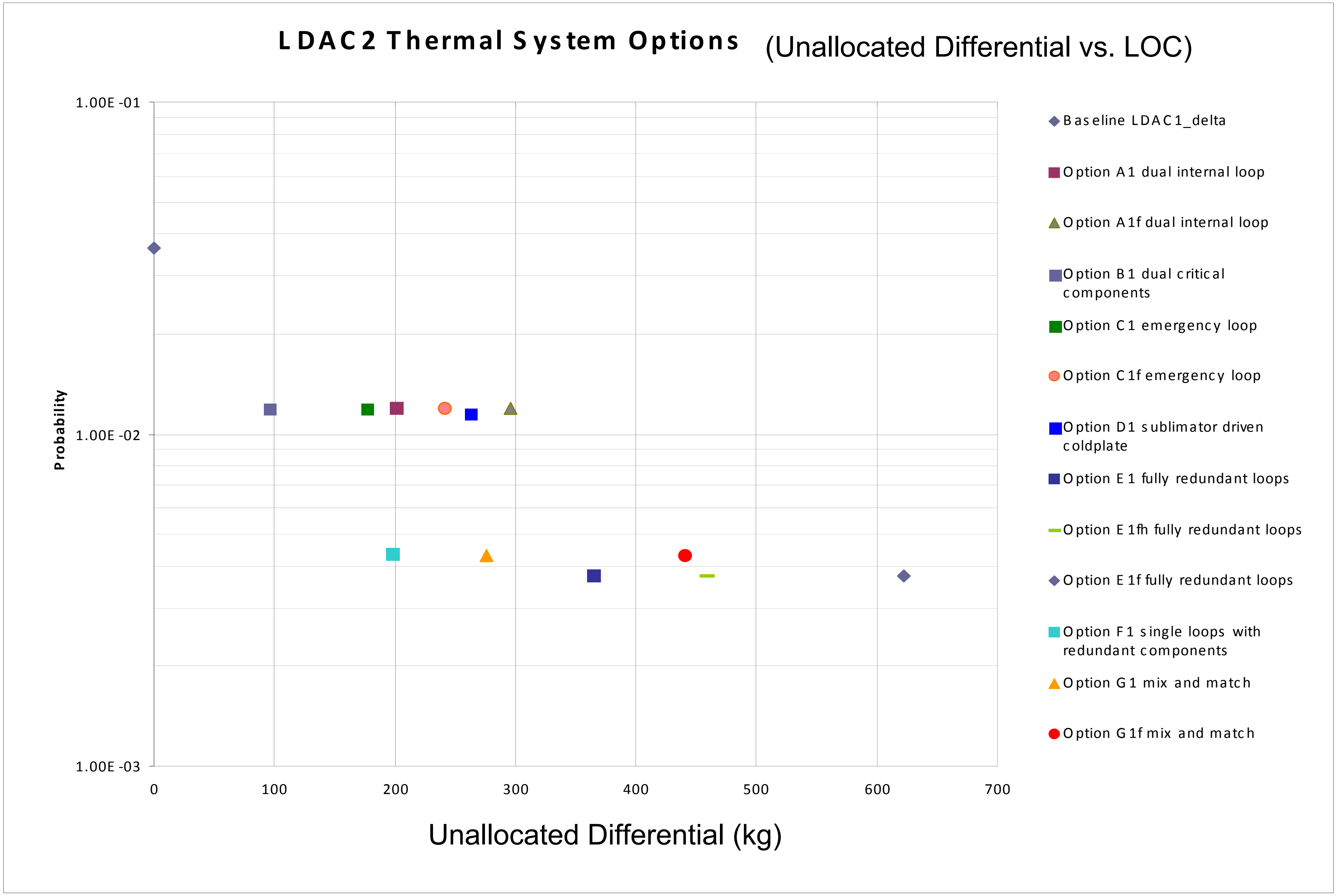
Graphical Summary of Options



Top Contenders:

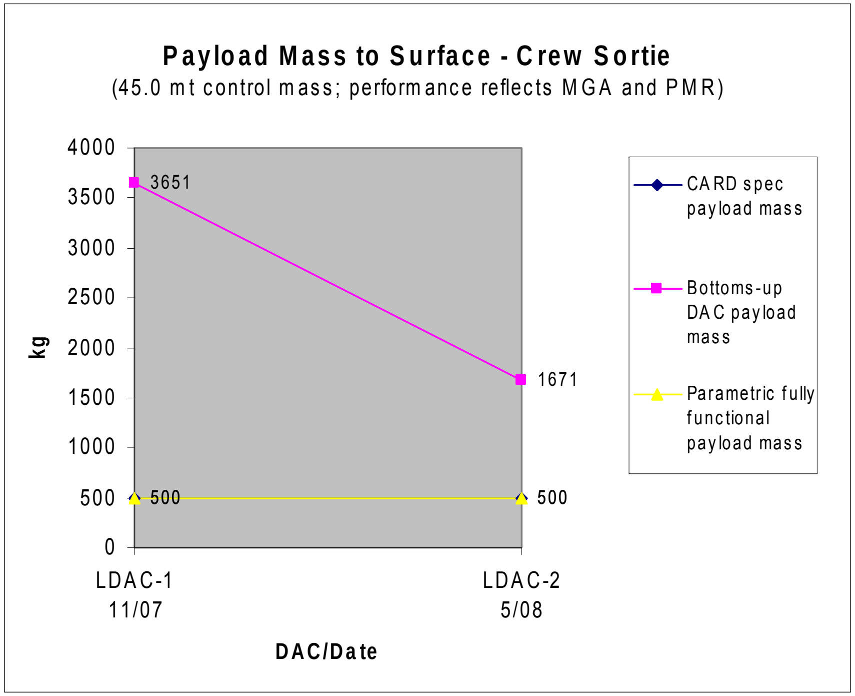
Option	Mass (Kg)	LOM	LOC	LOM		LOC	LxC
(C) - Dissimilar SV	23.95	5.45E-03	6.86E-06	1 in	183	145698	1x5
(E3) - Full + XPDR&SDR (w/o x-stp)	27.06	4.70E-03	6.62E-05	1 in	213	15117	2x5
(E2) - Full + XPDR (w/o x-stp)	31.65	1.42E-04	1.06E-04	1 in	7023	9435	3x5
(B2) - ByPass (IFM)	22.23	3.97E-03	1.94E-04	1 in	252	5143	3x5

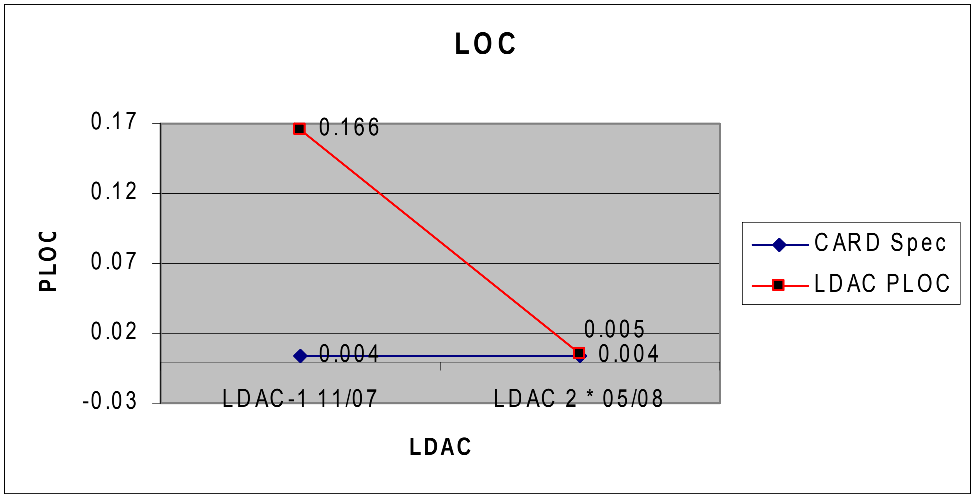
Another Example: Active Thermal



LDAC-2 Overview

- The initial Lander Design and Analysis Cycles (May-November 2007) created a “minimal functionality” lander design that serves as a baseline upon which to add safety, reliability and functionality back into the design with known changes to performance, cost and risk.
- LDAC-2 completed in May 2008. Goal was to “buy down” Loss of Crew (LOC) risks.
- “Spent” approximately 1.3 t to buy down loss of crew (LOC) risks.
- “Spent” an additional 680kg on design maturity.





* Note: Based on simplified models that address identified risks.

Lessons Learned During Risk Buy-down

- **Full redundancy was usually heaviest, frequently NOT most effective for improving LOC**
  - Conclusion may be different for LOM
- **Quantitative risk tool was necessary to <u>inform</u> good design decisions**
  - Always necessary to correlate engineering judgment with tool results
  - Tool forces team to reconsider
  - However, cannot rely solely on tool results. Must be able to technically explain decision.
- **A risk tool the designers can interact with is a significant aid – improves tool and design**
  - e.g., when a result did not correlate with engineering experience, designers could easily understand model in tool. Sometimes changed model and sometimes did not.
- **Designing for minimum risk**
  - results in lower weight design
  - is much harder and time consuming than simply adding redundancy
  - **But, design team ends up much more intelligent on risk and design drivers**
- **Design for Minimum Risk is the way to go if you are trying to build a smart design team**